Docker

Todo

1. Clona el projecte https://gitlab.com/xtec/asix-11

```
box@nmap:~$ git clone https://gitlab.com/xtec/asix-11/
Cloning into 'asix-11'...
warning: redirecting to https://gitlab.com/xtec/asix-11.git/
remote: Enumerating objects: 370, done.
remote: Counting objects: 100% (370/370), done.
remote: Compressing objects: 100% (219/219), done.
remote: Total 370 (delta 176), reused 290 (delta 124), pack-reused 0
Receiving objects: 100% (370/370), 264.51 KiB | 3.53 MiB/s, done.
Resolving deltas: 100% (176/176), done.
box@nmap:~$ ls
asix-11
```

2. Importa el projecte i arrenca el docker-compose que està a la carpeta **`asix-11/nginx`**:

```
box@nmap:~/asix-11/nginx$ docker-compose up -d
  Starting nginx_minio_4_1            ... done
  Starting nginx_cryptpad_1           ... done
  Starting nginx_wordpress_database_1 ... done
  Starting nginx_minio_2_1            ... done
  Starting nginx_minio_1_1            ... done
  Starting nginx_minio_3_1            ... done
  Starting nginx_etherpad_mariadb_1   ... done
  Starting nginx_wordpress_1          ... done
  Starting nginx_etherpad_1           ... done
  Starting nginx_proxy_1              ... done
box@nmap:~/asix-11/nginx$
```

3. Fes un **`nmap`** de la interficies **`enp0s8`** per veure els serveis que estan disponibles:

```
box@nmap:~$ ip -brief addr | grep enp0s8
enp0s8           UP             192.168.56.18/24 fe80::a00:27ff:fe62:675d/64
box@nmap:~$
box@nmap:~$ nmap -p- 192.168.56.18
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-20 09:27 UTC
Nmap scan report for nmap (192.168.56.18)
Host is up (0.00025s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
8001/tcp open  vcom-tunnel
8002/tcp open  teradataordbms
8005/tcp open  mxi
9000/tcp open  cslistener
9001/tcp open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
box@nmap:~$
```

4. Verifica. Obre el navegador a algun d'aquests ports per veure que hi ha:

Escaneja un host

1. Crea una nova sessió interactiva al contenidor **`nginx_etherpad_mariadb_1`** i **instal.la `nmap`**:

```
box@nmap:~$ docker exec -it nginx_etherpad_mariadb_1 bash
root@a0d83da0097e:/#
root@a0d83da0097e:/# apt update && apt install -y nmap
```

2. Fes un escaner local:

```
root@a0d83da0097e:/# nmap -p- localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-20 09:33 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000024s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65534 closed ports
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 2.79 seconds
root@a0d83da0097e:/#
```

Pots veure que **el port `3306/tcp` està obert** — és on la base de dades està escoltant ("listening").

Escaneja una xarxa

1. Descobreix quina adreça tens:

```
root@a0d83da0097e:/# ip -f inet -4 -o addr
1: lo    inet 127.0.0.1/8 scope host lo\       valid_lft forever p
46: eth0    inet 172.20.0.2/16 brd 172.20.255.255 scope global eth
root@a0d83da0097e:/#
```

2. Fes un escaneix de la xarxa local:

```
root@a0d83da0097e:/# nmap -p- -T5 172.20.0.2/28
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-20 09:45 UTC
Nmap scan report for nmap (172.20.0.1)
Host is up (0.000046s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
8001/tcp open  vcom-tunnel
8002/tcp open  teradataordbms
8005/tcp open  mxi
9000/tcp open  cslistener
9001/tcp open  tor-orport
MAC Address: 02:42:8E:B2:50:50 (Unknown)

Nmap scan report for nginx_etherpad_1.nginx_etherpad (172.20.0.3)
Host is up (0.000094s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
9001/tcp open  tor-orport
MAC Address: 02:42:AC:14:00:03 (Unknown)

Nmap scan report for a0d83da0097e (172.20.0.2)
Host is up (0.000019s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 16 IP addresses (3 hosts up) scanned in 11.18 seconds
root@a0d83da0097e:/#
```

Exercici

Escaneja totes les xarxes de `nginx_` i descriu la seva topologia.

1. Fes servir docker ps per veure quines són.

```
CONTAINER ID   NAMES                          PORTS
ed2f110c63d4   nginx_proxy_1                  0.0.0.0:8001-8002->8001-8002/tcp, ::
:8001-8002->8001-8002/tcp, 0.0.0.0:8005->8005/tcp, :::8005->8005/tcp, 80/tcp, 0.
0.0.0:9000-9001->9000-9001/tcp, :::9000-9001->9000-9001/tcp
48e880580cf7   nginx_etherpad_1               9001/tcp
33964e509198   nginx_wordpress_1              80/tcp
a9b150a516f3   nginx_cryptpad_1               3000-3001/tcp
52240657e276   nginx_wordpress_database_1     3306/tcp, 33060/tcp
916f7f14fe12   nginx_etherpad_mariadb_1       3306/tcp
efecfb804440   nginx_minio_4_1                9000/tcp
2e4a5177fd8a   nginx_minio_2_1                9000/tcp
0bed0786a016   nginx_minio_3_1                9000/tcp
3348159e66c0   nginx_minio_1_1                9000/tcp
box@nmap:~/asix-11/nginx$
```

2. Escaneja tres xarxes de **`nginx_`** i descriu la seva topologia.

   Tingues en compte que alguns contenidors:

- No tenen bash. Per tant, enlloc de **`/bin/bash`** has d'utilitzar **`/bin/sh`**
- No utilitzen `apt` sinó apk: `apk update && apk add -y nmap`

Traceroute

Escaneja a www.nytimes.com amb l'opció `--traceroute` i explica la informació que has trobat:

```
box@nmap:~$ sudo nmap -PN -T4 --traceroute www.nytimes.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-20 14:18 UTC
Nmap scan report for www.nytimes.com (151.101.133.164)
Host is up (0.023s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   3.06 ms  _gateway (192.168.1.1)
2   6.85 ms  167.red-81-46-38.customer.static.ccgg.telefonica.net (81.46.38.16
3   6.88 ms  213.red-81-46-34.customer.static.ccgg.telefonica.net (81.46.34.21
4   6.90 ms  41.red-81-46-44.customer.static.ccgg.telefonica.net (81.46.44.41)
5   6.93 ms  1.red-80-58-78.staticip.rima-tde.net (80.58.78.1)
6   12.23 ms gi0-4-1-5-gramiabr4.net.telefonicaglobalsolutions.com (216.184.11
7   ...
8   13.15 ms 151.101.133.164

Nmap done: 1 IP address (1 host up) scanned in 9.35 seconds
box@nmap:~$
```

Encara que el "New York Times" és un diari de Nova York (Estats Units) el seu servidor està molt aprop.

GeoIP

1. Instal.la el paquet **geoip-bin**.
2. Mirem on està la IP:

```
box@nmap:~$ geoiplookup 151.101.133.16
GeoIP Country Edition: ES, Spain
box@nmap:~$
```

Això vol dir que **New York Times** està fent servir un **CDN.**

3. Si volem informació més exacta hem d'instal.lar unes bases de dades GeoIP:

```
sudo add-apt-repository -y ppa:maxmind/ppa
```

```
sudo apt update && sudo apt install -y geoipupdate mmdb-bin
```

4. Executa aquesta comanda per crear el fitxer GeoIP.conf (donarà error, no passa res):

```
box@suricata:~$ sudo geoipupdate -v
Error loading configuration: invalid account ID format
box@suricata:~$
```

5. Edita el fitxer `/etc/GeoIP.conf` i configura l'`AccountID` i la `LicenseKey`:

```
AccountID 800171
LicenseKey FYDHhBlgkLwgwL25
```

```
  GNU nano 6.2                          /etc/GeoIP.conf *
# Please see https://dev.maxmind.com/geoip/updating-database
# instructions on setting up geoipupdate, including informat
# download a pre-filled GeoIP.conf file.

# Replace YOUR_ACCOUNT_ID_HERE and YOUR_LICENSE_KEY_HERE wit
# ID and license key combination associated with your MaxMin
# are available from https://www.maxmind.com/en/my_license_k
AccountID 800171
LicenseKey FYDHhBlgkLwgwL25
```

6. Actualitza la base de dades GeoIP:

```
box@nmap:~$ sudo geoipupdate -v
geoipupdate version 6.0.0-0+maxmind1~jammy (ubuntu-ppa) (linux-amd64)
Using config file /etc/GeoIP.conf
Using database directory /usr/share/GeoIP
```

7. Ja podem buscar en quina ciutat està la IP:

```
box@nmap:~$ file_city="/usr/share/GeoIP/GeoLite2-City.mmdb"
box@nmap:~$
box@nmap:~$ mmdblookup --file $file_city --ip 151.101.133.16 city names es

  "Madrid" <utf8_string>

box@nmap:~$
```

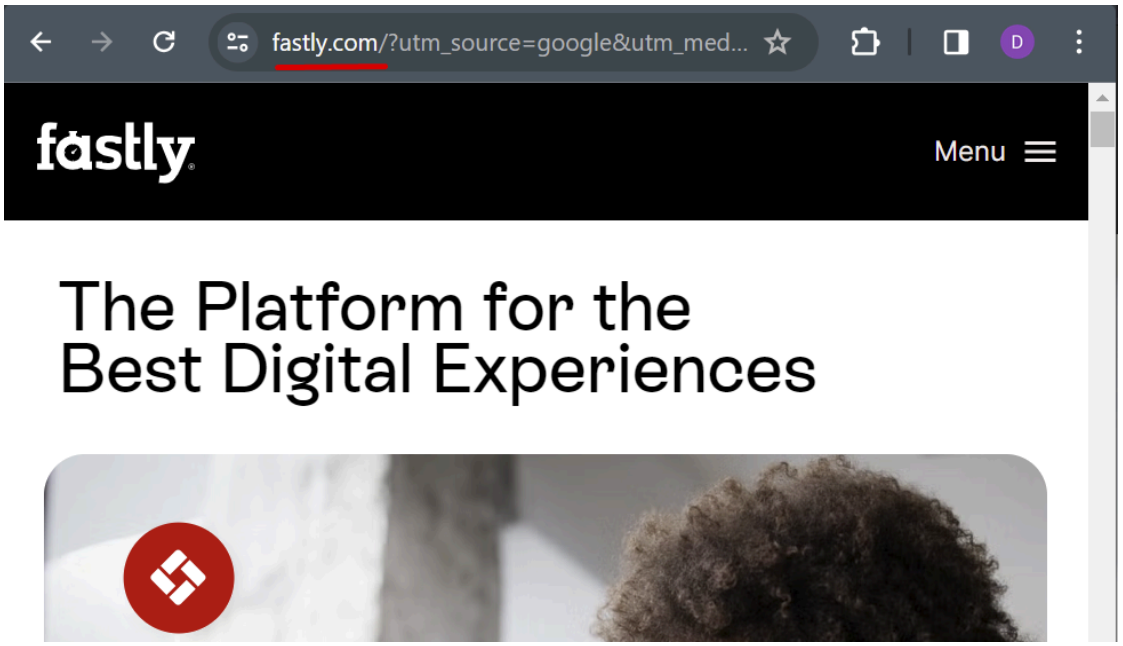
8. I de qui és aquesta IP ?

```
box@nmap:~$ whois 151.101.133.16 | head -20

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#


NetRange:       151.101.0.0 - 151.101.255.255
CIDR:           151.101.0.0/16
NetName:        SKYCA-3
NetHandle:      NET-151-101-0-0-1
Parent:         RIPE-ERX-151 (NET-151-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Fastly, Inc. (SKYCA-3)
box@nmap:~$
```

Tot el bloc d'IPs `151.101.0.0/16` les té Fastly, Inc.



Resum

"The New York Times" fa servir els serveis de **Fastly** per distribuir el seu lloc web.

Fastly té una xarxa de servidors distribuïts per tot el món, i quan em connecto a aquesta pàgina ho faig en un servidor a prop d'on estic:

Script

https://behacker.pro/como-utilizar-nmap-scripting-engine-nse/

Activitats

01 - Serveis

Escaneja els dominis que es llisten a continuació amb **`nmap -sV`** i explica els resultats obtinguts (ports, serveis, software que fan servir):

proven.cat , www.caixabank.es , www.mercadona.es

Solució:

```
box@nmap:~$ nmap -sV proven.cat
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-20 09:48 UTC
Nmap scan report for proven.cat (81.42.248.211)
Host is up (0.034s latency).
rDNS record for 81.42.248.211: 211.red-81-42-248.staticip.rima-tde.net
Not shown: 998 filtered ports
PORT    STATE SERVICE VERSION
80/tcp  open  http
443/tcp open  ssl/ssl Apache httpd (SSL-only mode)
1 service unrecognized despite returning data. If you know the service/v
```

Institut Provençana fa servir un servidor Apache.

Estás escanejant un servidor de l'Institut.

CaixaBank utilitzar els serveis de firewall i CDN de Cloudflare.

```
box@nmap:~$ nmap -sV www.caixabank.es
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-20 09:52 UTC
Nmap scan report for www.caixabank.es (172.64.155.160)
Host is up (0.015s latency).
Other addresses for www.caixabank.es (not scanned): 104.18.32.96 2606:4700:44
Not shown: 996 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          cloudflare
443/tcp  open  ssl/https     cloudflare
8080/tcp open  http-proxy    cloudflare
8443/tcp open  ssl/https-alt cloudflare
```

Estás escanejant els servidors de Cloudflare, no de CaixaBank.

Mercadona utilitza els serveis de CDN d'Akamai.

```
box@docker:~$ nmap -sV www.mercadona.es
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-21 10:33 UTC
Nmap scan report for www.mercadona.es (96.16.88.169)
Host is up (0.013s latency).
Other addresses for www.mercadona.es (not scanned): 96.16.88.166 2a02:26f0:e0::211:2572 2a02:26f0:e0::211
:255a
rDNS record for 96.16.88.169: a96-16-88-169.deploy.static.akamaitechnologies.com
Not shown: 997 filtered ports
PORT    STATE  SERVICE  VERSION
53/tcp  closed domain
80/tcp  open   http     AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
443/tcp open   ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.99 seconds
box@docker:~$
```

Estás escanejant els servidors d'Akamai, no de Mercadona.

02 - Traceroute

1. Escaneja a **china.org.cn** amb l'opció `--traceroute` i explica els resultats més rellevants:

```
box@nmap:~$ sudo nmap -PN -T4 --traceroute china.org.cn
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-20 15:11 UTC
Nmap scan report for china.org.cn (202.130.245.42)
Host is up (0.19s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
80/tcp   open     http
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
593/tcp  filtered http-rpc-epmap
4444/tcp filtered krb524

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   2.82 ms   _gateway (192.168.1.1)
2   5.75 ms   167.red-81-46-38.customer.static.ccgg.telefonica.net (81.46.38.167)
3   9.12 ms   217.red-81-46-34.customer.static.ccgg.telefonica.net (81.46.34.217)
4   ... 5
6   7.41 ms   be8-400-grtbcnes1.net.telefonicaglobalsolutions.com (213.140.50.218)
7   23.57 ms  176.52.249.63
8   76.85 ms  176.52.248.240
9   76.89 ms  219.158.38.105
10  191.86 ms 219.158.15.161
11  182.41 ms 219.158.3.145
12  ... 13
14  166.51 ms 114.245.244.54
15  160.85 ms 210.74.176.238
16  172.94 ms 202.130.245.226
17  179.57 ms 202.130.245.42

Nmap done: 1 IP address (1 host up) scanned in 42.97 seconds
box@nmap:~$
```

2. Anem a veure on estan les IPs …

```
box@nmap:~$ geoiplookup 176.52.249.63
GeoIP Country Edition: ES, Spain
box@nmap:~$ geoiplookup 176.52.248.240
GeoIP Country Edition: ES, Spain
box@nmap:~$ geoiplookup 219.158.38.105
GeoIP Country Edition: CN, China
box@nmap:~$ geoiplookup 202.130.245.42
GeoIP Country Edition: CN, China
box@nmap:~$
```

Hi ha un enllaç directe d'Espanya a China: 176.52.248.240 → 219.158.38.105 que només tarda 76.89 ms.

Amb la fibra òptica no importa gaire si dos nodes estan molt aprop o lluny: el temps es perd en els routers que han de processar els paquets.

Per tant, quants menys "salts" hagi de fer un paquet més ràpid arribarà.